SCOTT N. SCHOOLS (SC 9990)
Associate Deputy Attorney General
Acting United States Attorney

KYLE F. WALDINGER (ILSB 6238304)
Assistant United States Attorney

450 Golden Gate Avenue, 11th Floor
San Francisco, California 94102
Telephone: (415) 436-6830
Facsimile: (415) 436-7234

Attorneys for Plaintiff

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

UNITED STATES OF AMERICA, Plaintiff, v. DAVID NOSAL, Defendant.	No. CR 08-0237 MHP **UNITED STATES' OPPOSITION TO DEFENDANT NOSAL'S SECOND MOTION TO DISMISS INDICTMENT** Hrg. Date: February 17, 2009 Time: 10:00 a.m. Crtrm. 15: Hon. Marilyn Hall Patel

TABLE OF CONTENTS

TABLE OF AUTHORITIES

FEDERAL CASES

STATE CASES

FEDERAL STATUTES

STATE STATUTES

FEDERAL RULES

SCOTT N. SCHOOLS (SC 9990)
Associate Deputy Attorney General
Acting United States Attorney

KYLE F. WALDINGER (ILSB 6238304)
Assistant United States Attorney

450 Golden Gate Avenue, 11th Floor
San Francisco, California 94102
Telephone: (415) 436-6830
Facsimile: (415) 436-7234

Attorneys for Plaintiff

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

UNITED STATES OF AMERICA, Plaintiff, v. DAVID NOSAL, Defendant.	No. CR 08-0237 MHP **UNITED STATES' OPPOSITION TO DEFENDANT NOSAL'S SECOND MOTION TO DISMISS INDICTMENT** Hrg. Date: February 17, 2009 Time: 10:00 a.m. Crtrm. 15: Hon. Marilyn Hall Patel

INTRODUCTION

The defendant David Nosal has filed a second motion seeking to dismiss the Superseding Indictment ("Indictment"). The Court should deny the defendant's motion in its entirety.

Much of the defendant's motion relies on a mischaracterization of the charged offenses, as well as a failure to squarely address the allegations that knock the legs out from under his arguments. For example, Nosal argues that Counts Two through Nine "only" allege "misappropriation" on behalf of Christian & Associates, and that the unauthorized computer access alleged in those charges "merely breaches a contract conditioning access." *See* Def. Mtn., at 3–8. In truth, however, Counts Two through Nine allege that the defendant and others fraudulently accessed the computer system of his former employer Korn/Ferry International ("Korn/Ferry") on specific dates for the purpose of obtaining valuable information. Those charges do *not* allege that the defendant and others merely misappropriated information that they

happened already to have in their possession. In addition, the Indictment is clear that these actions were taken for the purpose of assisting *Nosal* in his executive search activities (and were not merely for the benefit of Christian & Associates). Further, the Indictment relates to much more than a breach of an agreement relating to computer use. Rather, the case relates to a scheme — fraudulent from bark to core — to steal confidential and proprietary information from Korn/Ferry's computer system.

The defendant also mischaracterizes the trade secret charges alleged in Counts Ten and Eleven. Those charges do *not* relate, as Nosal claims, to "the same instance of conduct." *Id.* at 10:17–18. On the contrary, as the allegations in the Indictment make clear, the criminal acts alleged in Counts Ten and Eleven occurred at different times on April 12, 2005. Moreover, each charge pertains to different conduct (essentially, theft and copying on the one hand versus receipt and possession on the other), and each charge relates to differing sets of data. Accordingly, Counts Ten and Eleven are not multiplicitous, because each requires proof of an additional fact that the other does not.

With respect to the *mens rea* requirement of Counts Ten and Eleven, the defendant incorrectly states the court's holdings in *United States v. Krumrei* and *United States v. Hsu*. Neither of those cases "determined" that the Economic Espionage Act (EEA) "must be interpreted to include an additional mens rea element [of knowledge of illegality] that is not specified in the statutory text," *id.* at 9:19–21, as the defendant argues. Rather, the cases simply upheld void-for-vagueness challenges to the EEA; neither announced a rule of pleading.

Finally, in arguing that the mail fraud charges are based merely on an "undisclosed breach" of contract, *id.* at 12:7–9 & 12:23 – 26, the defendant largely ignores the allegations that the defendant devised and participated in a scheme to defraud Korn/Ferry of $25,000 per month (as well as other payments) and of information in Korn/Ferry's computer system, and that he did so by making affirmative misrepresentations to Korn/Ferry on a regular basis, by using a fictitious name in his business dealings, and by stealing proprietary and confidential information from Korn/Ferry's computer system, among other actions. Simply put, the Indictment's mail fraud charges are based on much more than Nosal's "undisclosed breach" of contract.

ARGUMENT

I. DISMISSAL OF INDICTMENTS IS GENERALLY DISFAVORED.

In this case, the defendant seeks an order dismissing each and every one of the charges against him. However, "[t]he dismissal of an indictment is considered a 'drastic step' and is generally disfavored as a remedy." *Guam v. Muna*, 999 F.2d 397, 399 (9th Cir. 1993) (quoting *United States v. Rogers*, 751 F.2d 1074 (9th Cir. 1985)).

The pleading standards with which the government must comply are well known: Rule 7(c) provides in relevant part that an indictment shall contain a "plain, concise, and definite written statement of the essential facts constituting the offense charged." Fed. R. Crim. P. 7(c). In order to be legally sufficient, an indictment must contain the elements of the offense charged, fairly inform the defendant of the charge, and enable the defendant to plead double jeopardy as a defense to future prosecution for the same offense. *See Hamling v. United States*, 418 U.S. 87, 117 (1974); *United States v. Fernandez*, 388 F.3d 1199, 1217–18 (9th Cir. 2004). Under Ninth Circuit law, an indictment need do little more than track the language of the statute, include "implied, necessary elements, not present in the statutory language," and state the approximate time and place of the alleged crime. *See United States v. Jackson*, 72 F.3d 1370, 1380 (9th Cir. 1995); *United States v. Tavelman*, 650 F.2d 1133, 1137 (9th Cir. 1981).

With these principles in mind, the government turns to the defendant's various arguments in support of his motion to dismiss the Indictment.

II. COUNTS TWO THROUGH NINE PROPERLY ALLEGE THAT THE DEFENDANT ACCESSED KORN/FERRY'S COMPUTER SYSTEM WITHOUT AUTHORIZATION, AND IN EXCESS OF AUTHORIZED ACCESS.

The defendant argues that Counts Two through Nine of the Indictment must be dismissed because the statutory provision under which they are brought — 18 U.S.C. § 1030(a)(4) — does not encompass the facts of this case, *i.e.*, the use of a Korn/Ferry employees' usernames and passwords to access Korn/Ferry's computer system for the purpose of obtaining information to be used in the defendant Nosal's competing business. As set forth in more detail below, the defendant's proffered interpretation of Section 1030(a)(4) is not supported by common sense, or by the weight of authority.

A. Summary of Counts Two through Nine of the Indictment.

Counts Two through Nine charge the defendant David Nosal with accessing with the intent to defraud the computer system of Korn/Ferry — without authorization and in excess of authorized access — and obtaining something of value as a result of such access.

Counts Two through Nine incorporate the introductory allegations in the Indictment set out in ¶¶ 1–11, as well as the allegations regarding the charged conspiracy set out in ¶¶ 13–19. As such, those counts allege that the defendant was employed at the executive search firm Korn/Ferry International until October 2004. Indictment, ¶ 2. After he left Korn/Ferry, Nosal was assisted in setting up his own executive search firm by his co-defendant Becky Christian (who left Korn/Ferry's employment in January 2005), by an individual identified as "M.J." (who left Korn/Ferry's employment in March 2005), and by an individual identified as "J.F." (who left Korn/Ferry's employment in August 2005). *Id.*, ¶¶ 3–5.

The Indictment contains numerous allegations regarding Korn/Ferry's computer system and the confidentiality of the information contained therein. Significantly, the Indictment alleges that Korn/Ferry employees "received unique usernames and created passwords for use on the company's computer systems," which were intended to be used by the Korn/Ferry employee only. Indictment, ¶ 9. The Indictment also alleges that Nosal, Christian, M.J., and J.F. each entered into a confidentiality agreement with Korn/Ferry. Each agreement explained that the information in Korn/Ferry's computer system was owned by Korn/Ferry, and restricted the use and disclosure of all information, except for legitimate Korn/Ferry business. *Id.*, ¶ 10. Finally, each time a Korn/Ferry employee logged onto the computer system, he was informed that he needed "specific authority to access any Korn/Ferry system or information." Indictment, ¶ 11.

The charges in Counts Two through Nine relate to instances in which the Korn/Ferry computer user account of Christian or J.F. was used to access Korn/Ferry's computer system to obtain information regarding potential candidates for corporate executive positions, which information was to be used in Nosal's competing business. The Indictment alleges that these instances of access were performed by individual conspirators (1) "prior to and upon termination of their employment with Korn/Ferry by using their own Korn/Ferry" credentials, and (2) after

their separation from Korn/Ferry by using — either directly or through J.F. — J.F.'s Korn/Ferry credentials. *See* Indictment, ¶¶ 16–17. The government expects to prove that (1) Christian used her own credentials to access Korn/Ferry's computer system in the instance alleged in Count Two; (2) Christian used J.F.'s credentials to access the computer system in the instance alleged in Count Three; (3) Christian asked J.F. to access the computer system in the instances alleged in Counts Four, Seven, and Eight; (4) M.J. asked J.F. to access the computer system in the instances alleged in Counts Five and Six; and (5) M.J. used J.F.'s credentials to access the computer system in the instance alleged in Count Nine.[1]

The government will present evidence that Nosal directed Christian, M.J., and J.F. to obtain information from Korn/Ferry's computers, and that he entered into a conspiracy with those individuals to access Korn/Ferry's computer system for that purpose.[2]

/ / /

---

[1]The defendant's motion incorrectly suggests that the Indictment alleges only that "the defendants gained access to the Korn/Ferry computers '*by using their own Korn/Ferry user names and passwords*.'" Def. Mtn., at 8 (quoting Indictment, ¶ 16) (emphasis in defendant's motion). However, he ignores the next paragraph of the Indictment, which alleges that the conspirators *also* gained access to Korn/Ferry's computer system "by using, either *directly* or through J.F., J.F.'s Korn/Ferry username and password." Indictment, ¶ 17 (emphasis added). Given that J.F.'s password was used on at least two occasions by someone other than J.F. to access Korn/Ferry's computer system (*e.g.*, Counts Three and Nine), even the defendant apparently would concede that those counts properly allege unauthorized access to Korn/Ferry's computer system, since they relate to access to that computer system by an outsider.

[2]In labeling this prosecution an "expansive theory of liability," Def. Mtn., at 4 n.3, Nosal fails to acknowledge other prosecutions employing such a theory, including one in this Court. *See, e.g.*, *United States v. Zenaida Smith*, CR 07-0246 MHP; *United States v. Robinson*, CR 07-0596 JF; *United States v. Williams et al.*, CR 04-40018 CW. Thus, far from representing an "expansive" theory, this case represents a typical criminal action brought under Section 1030. Indeed, the CFAA was enacted in an effort to create an omnibus criminal statute to address computer-related crimes. S. Rep. 104-357, 104th Cong., 2d Sess. 5 (1996) ("the Computer Fraud and Abuse statute facilitates addressing in a single statute the problem of computer crime, rather than identifying and amending every potentially applicable statute affected by advances in computer technology"). "Section 1030 is general." *United States v. Mitra*, 405 F.3d 492, 495 (7th Cir. 2005). As technology changes, the effective scope of Section 1030 may grow, but this does not mean that the statute should be given "less coverage than its language portends." *Id.*

B. The Defendant's Liability for the Offenses Alleged in Counts Two through Nine.

Before turning to the defendant's substantive arguments regarding Counts Two through Nine, the government first addresses the various comments made in the defendant's brief questioning how he could possibly be liable for actions that are alleged in the Indictment to have been taken by others. *See, e.g.*, Def. Mtn., at 8:18–27 ("The indictment does not allege that Mr. Nosal himself ran any searches using J.F.'s password, nor does it allege that he assisted anyone else in doing so."); *cf. also id.*, at 11 n.6 (arguing that Count Ten does not properly allege an offense because it does not allege that trade secrets were stolen "by Mr. Nosal himself"). The defendant fails to consider familiar principles of criminal liability.

Here, the Indictment alleges liability in Counts Two through Nine under both the substantive statutes and 18 U.S.C. § 2. Section 2 "eliminates the common law distinction between 'principal' and 'accessory' and makes one who aids and abets or causes the commission of a crime punishable as a principal." *United States v. Armstrong*, 909 F.2d 1238, 1241 n.1 (9th Cir. 1989). All indictments are read to embody this statute. *See United States v. Vaanderling*, 50 F.3d 696, 702 (9th Cir. 1995). Section 2 provides criminal liability for a defendant who "aids, abets, counsels, commands, induces or procures" the commission of an offense or who "willfully causes an act to be done which if directly performed by him or another would be an offense against the United States." Thus, Nosal may be found guilty of the Indictment's substantive crimes, even if he did not personally commit the acts constituting those crimes, but aided and abetted in their commission. Indeed, Nosal's co-conspirators have admitted in their plea colloquys that Nosal directed them to take items from Korn/Ferry's computer system. *See, e.g.*, Plea Agrm., ¶ 2, CR 07-0568 MHP ("I also understood [Nosal] to be directing me to take from Korn/Ferry whatever I thought would be necessary or helpful for [Nosal's] new company. . . ."); Plea Agrm., ¶ 2, CR 07-0337 MHP ("[Nosal] asked me to retrieve position specifications for a particular job function from Korn/Ferry's computer system.").

Nosal can also be found guilty under the law of conspiracy because

> [e]ach member of the conspiracy is responsible for the actions of the other conspirators performed during the course and in furtherance of the conspiracy. If one member of a conspiracy commits a crime in furtherance of a conspiracy, the

other members have also, under the law, committed that crime. . . .

9th Cir. Model Jury Instr., 8.20. This so-called "*Pinkerton*" charge

> derives its name from *Pinkerton v. United States*, 328 U.S. 640 (1946), which held that a defendant could be held liable for a substantive offense committed by a co-conspiration as long as the offense occurred within the course of the conspiracy, was within the scope of the agreement, and could reasonably have been foreseen as a necessary or natural consequence of the unlawful agreement.

9th Cir. Model Jury Instr., 8.20, comment (citation omitted). Because Count One of the Indictment alleges that Nosal entered into a conspiracy to commit computer fraud, and because the instances alleged in Counts Two through Nine were crimes committed as part of that conspiracy, Nosal can be liable under a *Pinkerton* theory for those crimes.

C. Counts Two through Nine Properly Allege that the Defendant Accessed Korn/Ferry's Computer System Without Authorization, and in Excess of Authorized Access.

The defendant first argues that the statute under which Counts Two through Nine are brought — Section 1030(a)(4) of the Computer Fraud and Abuse Act (CFAA) — prohibits only "unauthorized access" or "exceeding authorized access" and that it does not prohibit "misappropriation." The gravamen of the defendant's argument is that employees who are given physical and electronic access to their employer's computer systems, and who then steal information that might be available to them pursuant to that access, cannot be found to have accessed those computer systems without authorization (or to have done so in excess of their authorized access). The defendant's argument fails on several grounds.

As an initial matter, the defendant's argument that Section 1030(a)(4) does not "cover" misappropriation misses the mark. Notably, in quoting what he argues is the "relevant part" of Section 1030(a)(4), the defendant states only that the statute "'makes it a crime for a person to 'knowingly and with intent to defraud, access[] a protected computer without authorization, or exceed[] authorized access.'" Def. Mtn., at 3 (quoting Section 1030(a)(4)). The defendant fails, however, to cite the *other* elements set out in the statute, namely, that the defendant "further[] the intended fraud and *obtain[] anything of value*." 18 U.S.C. § 1030(a)(4) (emphasis added). Accordingly, whatever term one applies — "misappropriation" or "obtaining anything of value" — the statute clearly covers situations in which information is taken from a computer system.

Indeed, the statute *requires* the government to prove that something was taken; mere "access" to a computer system is not enough to trigger liability. Accordingly, the Indictment's allegations that items were taken from Korn/Ferry is part and parcel of a Section 1030(a)(4) charge.

Second, Counts Two through Nine allege that Nosal is culpable for having accessed Korn/Ferry's computer system on eight dates *after* his separation from Korn/Ferry in October 2004. Accordingly, even assuming that the Korn/Ferry employee user accounts of Christian and J.F. were used by those individuals to obtain information at a time when they were still employed at Korn/Ferry, the Indictment alleges those items were obtained for the purpose of assisting Nosal and his co-conspirators in their own business activities. *See* Indictment, ¶ 18. Clearly, if an individual *steals* the password of a competitor's employee and thereafter fraudulently accesses that competitor's computer system and obtains something of value using that password, such access would be "without authorization" under Section 1030, regardless of whether the employee from whom he stole the password was otherwise "authorized" to do so. Under the defendant's theory, however, if that same individual *paid* the competitor's employee to access the competitor's computer systems and obtain information, there would be no "unauthorized access," regardless of whether the employee's actions violated his agreements with, or duty of loyalty to, his employer. This result is not consistent with a fair reading of the statute.

Third, although some courts have held that Section 1030 does not cover an employee's access to his employer's computer system using log-in credentials provided to him by that employer, the weight of authority supports the opposite view. Notably, the only federal *appellate* courts to have ruled on this issue have agreed with the government's interpretation of the statute.[3] For example, in *International Airport Centers, L.L.C. v. Citrin*, 440 F.3d 418 (7th Cir. 2006), the Seventh Circuit held that employees who access their employer's computers to obtain or delete business information for their own personal benefit or the benefit of a competitor act "without authorization" or "exceed authorization" within the meaning of the statute. *See Citrin*, 440 F.3d

[3]Section 1030(g) provides for a civil cause of action for violations of Section 1030. Because of that provision, many of the cases construing Section 1030 have arisen in the civil, as opposed to the criminal, context.

at 420–21 (finding employee acted without authorization because the employee's "breach of his duty of loyalty [in deleting computer files] terminated his agency relationship . . . and with it his authority to access the laptop"). As the Seventh Circuit recognized, even when "authorization" exists, it can be withdrawn or can lapse under well-accepted principles of agency law. *See also Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc.*, 119 F. Supp.2d 1121, 1124 (W.D. Wash. 2000) (finding that insiders with authorization to use a system can lose that authorization when they act as agents of an outside organization).[4]

Similarly, in *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577 (1st Cir. 2001), the First Circuit held that a former employee of a travel agent could be found to have exceeded his authorization to obtain information from his former employer's website because, in violation of his confidentiality agreement with the employer, he used confidential information he had obtained as an employee to create a program that enabled his new travel company to obtain information from that website that he could not have obtained as efficiently without the use of that confidential information. *Id.* at 583–84.

Further, although the question at issue here was not directly addressed in the case, the Ninth Circuit upheld a jury verdict on behalf of a plaintiff in a civil action brought under Section 1030 where one of the allegations was that the defendant had

> hired away a [plaintiff's] employee who had given [the defendant] an unauthorized tour of the [plaintiff's] website. This employee, while still working for [the plaintiff], accessed confidential information regarding several thousand of [the plaintiff's] customers. He downloaded, and sent to his home email account, the confidential address to [the plaintiff's website's] server so that he could access the server from home and retrieve customer lists.

Creative Computing v. Getloaded.com LLC, 386 F.3d 930, 932 (9th Cir. 2004); *id.* (noting that plaintiff prohibited competitors' access to its website). These facts are similar to those alleged in the instant case. *Cf. Theofel v. Farey-Jones*, 359 F.3d 1066, 1074 (9th Cir. 2004) (stating that use

---

[4]In *Shurgard*, employees were found to have acted "without authorization" when they accessed their employer's computers to obtain trade secrets for the benefit of a competitor. Applying principles of agency law, the court concluded that the employees' authorized access to the employer's computers ended when they became agents of the competitor. *Shurgard*, 119 F. Supp.2d at 1124–25.

of authorized third party's password by outside hacker to gain access to mail server fell within "the paradigm of what [Congress] sought to prohibit [under Stored Communications Act]").

Other appellate courts have upheld criminal convictions under Section 1030 where the theory of "unauthorized access" was based on the defendant's non-compliance with the intended function of the computer system at issue. For example, in the first appellate decision to use either term, the Second Circuit found that a defendant had gained "unauthorized access" to computers on "INTERNET" based on the fact that he did not use the features of the computer to which he did have access "in any way related to [those features'] intended function." *United States v. Morris*, 928 F.2d 504, 510 (2d Cir. 1991); *see also id.* at 511 (rejecting argument that Section 1030 was aimed only at "outsiders"); *United States v. Phillips*, 477 F.3d 215, 219–21 (5th Cir. 2007) (holding that evidence was sufficient to find defendant guilty of "unauthorized access" where defendant violated university's "acceptable use" computer policy and accessed portions of computer system he was never authorized to access under policy).

Several trial courts have agreed with the holdings reached in *Citrin*, *EF Cultural Travel*, and *Shurgard*. *See, e.g.*, *Hanger Prosthetics & Orthotics, Inc. v. Capstone Orthopedic, Inc.*, 556 F. Supp.2d 1122, 1131 (E.D. Cal. 2008) ("Both former employees and their new companies who seek a competitive edge through wrongful use of information from the former employer's computer system face liability under § 1030.") (citing *Pac. Aerospace & Elecs., Inc. v. Taylor*, 295 F. Supp.2d 1188 (E.D. Wash. 2003)); *ViCHIP Corp. v. Lee*, 438 F. Supp.2d 1087, 1100 (N.D. Cal. 2006) (rejecting employee's argument that his access to plaintiff's system was "technically authorized, since he deleted the [] files while still an officer and director"); *HUB Group v. Clancy*, 2006 WL 208684, at *3–*4 (E.D. Pa. Jan. 25, 2006) (holding that, if defendant accessed employer's database, not for use as an employee of that company, but for future use as competitor's employee, a violation of CFAA properly could be alleged); *cf. also Charles Schwab & Co. v. Carter*, 2005 WL 2369815, at *5–*7 (N.D. Ill. Sept. 27, 2005) (holding that if employee accessed computer user account for purpose of assisting future employer, liability could be established against employee and future employer under CFAA). *But see, e.g.*, *Lasco Foods, Inc. v. Hall & Shaw Sales*, 2009 WL 151687 (E.D. Mo. Jan. 22, 2009); *US Bioservices Corp. v. Lugo*,

2009 WL 151577 (D. Kan. Jan. 21, 2009); *Allied North Am. Ins. v. Woodruff-Sawyer*, 2005 WL 2354119 (N.D. Cal. 2005); Def. Mtn., at 4–6 (citing cases).

* * *

Courts typically analyze "the scope of a user's authorization to access a protected computer on the basis of the expected norms of intended use or the nature of the relationship established between the computer owner and the user." *Phillips*, 477 F.3d at 219. Based on a plain reading of the statute, common sense, and the case law authority cited above, this Court should conclude that an employee may act "without authorization" or "in excess of authorized access" when he accesses his employer's computers (which he has permission to access) with the intent to defraud, or where, as here, he aids and abets, or is part of a conspiracy with, such an employee. *Cf. Shurgard*, 119 F. Supp.2d at 1126 ("'fraud' simply means wrongdoing and not proof of the common law elements of fraud"). In particular, the Court should reach that conclusion in this case based upon the detailed allegations regarding (1) the permitted uses of employee usernames and passwords at Korn/Ferry, *see* Indictment, ¶ 9; (2) the confidentiality agreements entered into between the conspirators and Korn/Ferry regarding the information in Korn/Ferry's computer system, *see id.*, ¶ 10; and (3) the notification given to employees each time that they logged onto Korn/Ferry's computer system, which stated that they needed "specific authority to access any Korn/Ferry system or information," *id.*, ¶ 11.[5]

For these reasons, and for all of the reasons set forth above, the defendant's motion to

---

[5]The defendant argues that, simply because "reasonable people could disagree about the scope of [Section 1030(a)(4)]," Def. Mtn., at 7, this Court should apply the "rule of lenity" and adopt *his* proffered interpretation. However, the rule of lenity is applicable only where "there is a grievous ambiguity or uncertainty in the language and structure of [an] Act, such that even after a court has seize[d] every thing from which aid can be derived, it is still left with an ambiguous statute." *Chapman v. United States*, 500 U.S. 453, 463 (1991) (second alteration in original, internal quotation marks and citations omitted); *see also United States v. Lanier*, 520 U.S. 259, 266 (1997) (noting that rule of lenity resolves ambiguity in criminal statutes). Here, the defendant does not argue that Section 1030 is ambiguous. As argued above, the government submits that the statute, plainly read, prohibits employees from using their usernames and passwords to access their employer's computers for the purpose of obtaining information to be used by a competitor. Because the statute is not ambiguous, the rule of lenity is inapplicable.

dismiss Counts Two through Nine (and the corresponding portions of the conspiracy charge in Count One) should be denied.

III. SECTION 1832 DOES NOT REQUIRE THAT THE INDICTMENT ALLEGE, OR THAT THE GOVERNMENT PROVE, THAT THE DEFENDANT HAD KNOWLEDGE THAT HIS ACTIONS WERE ILLEGAL.

The defendant next argues that Counts Ten and Eleven must be dismissed because they fail to allege that the defendant knew that his actions were illegal. However, proof that the defendant knew that his actions were illegal is not an element of the trade secret offenses charged in the Indictment.

A. The Economic Espionage Act and Its *Mens Rea* Requirements.

Counts Ten and Eleven of the Indictment are brought pursuant to 18 U.S.C. § 1832, which was enacted as part of the Economic Espionage Act (EEA). The EEA was enacted in part to protect our country's economic interests. As a House Report explained:

> For many years federal law has protected intellectual property through the patent and copyright laws. With this legislation, Congress will extend vital federal protection to another form of proprietary economic information — trade secrets. There can be no question that the development of proprietary economic information is an integral part of America's economic well-being.

H. Rep. No. 104-788, 104th Cong., 2d Sess. 4 (1996); *see also id.* (noting that "intangible assets have become more and more important to the prosperity of companies"). Although the defendant correctly notes that the EEA "'was not designed to punish competition, even when such competition relies on the know-how of former employees of a direct competitor,'" Def. Mtn., at 9 (quoting *United States v. Martin*, 228 F.3d 1 (1st Cir. 2000)), he does not complete the rest of the *Martin* court's description, *i.e.*, that the EEA *was* designed to prevent employees and their future employers "from taking advantage of confidential information gained, discovered, copied, or taken while employed elsewhere." *Martin*, 228 F.3d at 11. This distinction is not, as Nosal claims, "insolubly hazy." Def. Mtn., at 9. As *Martin* noted, the EEA specifically addresses situations, similar to the one here, in which a disgruntled employee walks out of his "company with a computer diskette full of engineering schematics." *Martin*, 228 F.3d at 11; *see also* S. Rep. 104-359, 104th Cong., 2d Sess. 6 (1996) ("A great deal of theft is committed by disgruntled individuals or employees who hope to harm their former company or line their own pockets.").

The three *mens rea* requirements set out in Section 1832(a) are that the defendant, "[*1*] with intent to convert a trade secret . . . to the economic benefit of anyone other than the owner thereof, and [*2*] intending or knowing that the offense will injure any owner of that trade secret, [*3*] knowingly" engages in misappropriation. "A knowing state of mind with respect to an element of the offense is (1) an awareness of the nature of one's conduct, and (2) an awareness of or a firm belief in or knowledge to a substantial certainty of the existence of a relevant circumstance, such as whether the information is proprietary economic information as defined by this statute." S. Rep. No. 104-359, at 16. Because criminal statutes covering the theft of tangible property generally require the government to provide that the defendant "[knew] that the object he [stole was] indeed a piece of property that he [had] no lawful right to convert for his personal use," the government generally must show that the defendant knew or had a firm belief that the information he or she was taking was a trade secret in cases brought pursuant to Section 1832 as well. 142 Cong. Rec. *S12213 (1996), 1996 WL 559474 (EEA legislative history); *see also United States v. Genovese*, 409 F. Supp.2d 253, 258 (S.D.N.Y. 2005) (discussing alleged circumstances that would indicate that EEA defendant knew the information was a trade secret).

It is well established, however, that ignorance of the law is no defense. The government need not prove that a defendant himself had concluded that the information he took fit the legal definition of a "trade secret" set forth in 18 U.S.C. § 1839(3). If the government had to prove this, Section 1832 violations would be nearly impossible to prosecute, and Congress's intent would be contravened:

> This [knowledge] requirement should not prove to be a great barrier to legitimate and warranted prosecutions. Most companies go to considerable pains to protect their trade secrets. Documents are marked proprietary; security measures put in place; and employees often sign confidentiality agreements.

142 Cong. Rec. *S12213 (1996), 1996 WL 559474. Based on this legislative history, the government can prove that a defendant knew that the information was a trade secret by proving that he was aware that it was protected by proprietary markings, security measures, and confidentiality agreements. *Id.* More generally, the government could simply prove that a defendant knew or had a firm belief that the information was valuable to its owner because it was

not generally known to the public, and that its owner had taken measures to protect it. On the other hand, a person could not be convicted under Section 1832 if he took a trade secret because of "ignorance, mistake, or accident." *Id.* Nor could he be convicted if "he actually believed that the information was not proprietary after [he took] reasonable steps to warrant such belief." *Id.*

B. Counts Ten and Eleven are Properly Pleaded.

In addition to the three *mens rea* elements explicitly set out in Section 1832, the defendant argues that this Court should read a *fourth* mental state requirement into the statute, *i.e.*, that the defendant knew his actions to be illegal. However, it is undisputed that Counts Ten and Eleven track the language of Section 1832 and that they duly incorporate all three of the *mens rea* elements set out in the statute. Moreover, it is undisputed that neither the Ninth Circuit nor any district court sitting in the Ninth Circuit has held that knowledge of illegality is an "implied, necessary element[]" of Section 1832. *See Jackson*, 72 F.3d at 1380.

As noted above, Section 1832 sets out a "knowing" *mens rea* requirement. The Supreme Court has held that, "unless the text of the statute dictates a different result, the term 'knowingly' merely requires proof of knowledge of the facts that constitute the offense." *Bryan v. United States*, 524 U. S. 184, 193 (1998); *see also United States v. Kafka*, 222 F.3d 1129, 1131 (9th Cir. 2000) (citing *United States v. Bostic*, 168 F.3d 718 (4th Cir. 1999), for proposition that "the term 'knowingly' as applied to section 922(g)(8) offenses does not require a defendant be aware of the illegality of his conduct"). In *Bryan*, the Supreme Court stated that "the term 'knowingly' does not necessarily have any reference to a culpable state of mind or to knowledge of the law." *Bryan*, 511 U.S. at 192. Rather, "the knowledge requisite to knowing violation of a statute is factual knowledge as distinguished from knowledge of the law." *Id.* at 192–93 (quoting *Boyce Motor Lines v. United States*, 342 U.S. 337, 345 (1952) (Jackson, J., dissenting)).

Notably, the *Bryan* Court dealt with a statute (Section 922) that included a "willful" element in the subsection at issue, but a "knowing" element in other subsections. Only the provision punishing willful violations required knowledge of illegality. The Court noted that, in order to establish a "willful" violation of a statute, the government must generally "prove that the defendant acted with knowledge that his conduct was unlawful" or that the defendant acted with

a "bad purpose." *Bryan*, 524 U.S. at 191–92 & n.12 (quoting, *e.g.*, *Ratzlaf v. United States*, 510 U.S. 137, 137 (1994)); *cf. also id.* at 198–200 (holding that "willfulness" element required only that government prove defendant's knowledge that the conduct was illegal, not that the government needed to prove the defendant had knowledge of the specific law or that he disregarded a known legal obligation). Based on *Bryan*, it would be a strange result to import a "willfulness" requirement into a statute (Section 1832) that clearly includes no such language and that, instead, sets forth the less-exacting *mens rea* requirement of "knowingly."

The defendant relies on a Sixth Circuit case and Pennsylvania district court case to argue that knowledge of illegality is an element of Section 1832 that must be pleaded and proved. *See* Def. Mtn., at 9–10 (citing *United States v. Krumrei*, 258 F.3d 535 (6th Cir. 2001) and *United States v. Hsu*, 40 F. Supp.2d 623 (E.D. Pa. 1999)). However, the cases relied upon by the defendant do not stand for the proposition he advances in his motion because those cases do not announce a rule of pleading. Neither *Krumrei* nor *Hsu* held that an indictment must contain an allegation that the defendant knew that his actions were illegal, nor did they hold that knowledge of illegality is an element of Section 1832. Rather, each court simply upheld the constitutionality of the EEA in the face of void-for-vagueness challenges, and each court did so after finding that the evidence showed that the defendant was aware that the information he stole was proprietary.

In *Krumrei*, the defendant argued on appeal that because the "reasonableness" of measures taken to maintain the confidentiality of a trade secret must be decided on a case-by-case basis, the entire statute was too vague to be enforced. *Krumrei*, 258 F.3d at 538; *see also id.* ("[D]efendant alleges that the lack of clarity as to what constitutes 'reasonable measures' has the potential to lead to arbitrary and discriminatory enforcement of the EEA."). In holding that Section 1832 was not unconstitutionally vague as applied to Krumrei, the Sixth Circuit found that there was sufficient evidence to show that he "was aware that he was selling confidential information to which he had no claim" and that he knew that the information that he took was proprietary to the company Wilsonart. *Id.* at 539. The court relied on statements made by the defendant at his guilty plea hearing, at which he admitted (1) obtaining trade secret information from his employer that he knew to be proprietary to Wilsonart, (2) forwarding the information to

a competitor of Wilsonart, and (3) taking his actions for the purpose of benefitting someone other than the owner of the trade secret. *Id.* Based on these concessions, the court found that Krumrei "cannot claim that the statute is vague when he clearly was aware that his actions fell within the activity proscribed by the statute." *Id.*

In *Hsu*, the defendant moved to dismiss a theft of trade secrets charge brought against him under Section 1832. As in *Krumrei*, the defendant in *Hsu* argued that Section 1832 was void for vagueness because the definition of "trade secret" does not define "'reasonable measures' to keep the information secret" or "what is meant by information not being 'generally known' or 'readily ascertainable' to the public." *Hsu*, 40 F. Supp.2d at 626. The district court held that Section 1832 was not void for vagueness as applied to Hsu because, based on evidence before the court, Hsu knew that the owner of the alleged trade secrets "had taken many steps to keep its technology to itself," *id.* at 628, and that the defendant could not acquire the technology by any other means than by getting it from a corrupt employee of the trade secret's owner, *id.* at 631.

Accordingly, neither the *Krumrei* holding nor the *Hsu* holding "determined" that the EEA included a knowledge-of-illegality element. *See* Def. Mtn., at 9:19–21.

* * *

Section 1832 makes it a crime to steal or otherwise misappropriate trade secrets. It does not regulate unusual financial transactions or obscure fraudulent business dealings. Theft, trafficking in stolen property, and possession of stolen property are common law concepts that every citizen is expected to understand. In this case, the Indictment alleges that the defendant knowingly stole and possessed trade secret information from Korn/Ferry's computer system that was (1) proprietary to Korn/Ferry, (2) the product of years of work by Korn/Ferry employees, (3) valuable, (4) protected by numerous security measures, (5) subject to confidentiality agreements, and (6) marked "Korn/Ferry Proprietary and Confidential." Indictment, ¶¶ 6–11. It further alleges that Nosal obtained that information through unauthorized access to Korn/Ferry's computer system, and that he obtained the information for the purpose of furthering his own economic interests. There is nothing about the nature of these crimes that suggests that Section 1832 must be read to include an element of knowledge of illegality. For all of these reasons, this

Court should deny the defendant's motion to dismiss Counts Ten and Eleven (and the corresponding portions of the conspiracy charge in Count One).

IV. COUNTS TEN AND ELEVEN ARE NOT MULTIPLICITOUS.

The defendant next argues that Counts Ten and Eleven of the Indictment should be dismissed because they are multiplicitous. In the alternative, the defendant argues that Count Ten is duplicitous. As set forth in more detail below, the defendant's multiplicity argument is without merit, and none of the defendant's arguments requires dismissal now of either count.

A. Legal Standard Regarding Multiplicitous Indictments.

Multiplicity arises when separate counts against a defendant charge the same offense. *United States v. Garlick*, 240 F.3d 789, 793–94 (9th Cir. 2001). "The test for multiplicity is whether each count 'requires proof of a[n additional] fact which the other does not.'" *Id.* at 794 (quoting *Blockburger v. United States*, 284 U.S. 299, 304 (1932) (alteration by *Garlick*)).

Contrary to the defendant's suggestion, multiplicity *does not* arise when a defendant is charged with two offenses related to the same underlying conduct. *See* Def. Mtn., at 10 ("The two counts are based on the same instance of conduct . . . ."). Congress may authorize cumulative punishments for separate criminal offenses that occur in the same act. *Albernaz v. United States*, 450 U.S. 333, 344 (1981). As set forth above, double jeopardy is not implicated, so long as each violation requires proof of an element that the other does not. *Blockburger*, 284 U.S. at 304.

B. Counts Ten and Eleven are not Multiplicitous.

The defendant contends that Counts Ten and Eleven are multiplicitous because they "are based on the same instance of conduct" and because "they are charged under subdivisions of Section 1832 that merely set out different means of committing the same offense." Def. Mtn., at 10. The defendant's argument fails for at least two reasons.

First, the defendant is wrong when he claims that Counts Ten and Eleven pertain to "the same instance of conduct." On the contrary, the two charges pertain to entirely different acts that occurred at different times. Count Ten relates to the *theft*, *copying* and *downloading* of *one* set of data from Korn/Ferry's computer system on April 12, 2005. *See* Indictment, Count Ten ("three

Korn/Ferry source lists" and referencing ¶ 19.b); *id.*, ¶ 19.b ("Each source list had been downloaded from the Searcher database earlier in the day on April 12, 2005 . . . ."). The government intends to show at trial that these source lists were downloaded on April 12 by Christian, after she had asked for and received J.F.'s username and password on April 11. *See id.*, ¶ 19.a ("On or about April 11, 2005, the defendant Christian sent an e-mail to J.F. stating 'It is to difficult to explain the searcher run I would need to log in as you.'").

In contrast, Count Eleven relates to the defendant's *receipt* and *possession* later in the day on April 12 of *two* sets of data. *See* Indictment, Count Eleven ("three Korn/Ferry source lists relating to prior searches for CFOs and information regarding CFOs that was 'cut and pasted' from a source list in Searcher" and referencing ¶¶ 19.b and 19.g). The Indictment alleges that the defendant came into the possession of the first set of data via an e-mail dated April 12. *See id.*, ¶ 19.b. The Indictment alleges that Nosal came into the possession of the second set of data via two other e-mails on the same day. *See id.*, ¶ 19.g. Thus, the defendant's argument regarding "the same instance of conduct" ignores the plain language of Counts Ten and Eleven.

The fact that there may be overlapping proof with respect to Counts Ten and Eleven does not mean that the counts are multiplicitous. *See United States v. Muhammad*, 120 F.2d 688, (7th Cir. 1997) (noting that, in determining multiplicity, "we focus on the statutory elements of the charged offenses, not the overlap in the proof offered to establish them, because a single act may violate several statutes without rendering those statutes identical"). Here, because each charge requires proof of a fact that the other does not, there is no multiplicity problem.

Second, the defendant's insistence that Congress intended only one penalty for violations of Section 1832's multiple subsections is belied by the statute's structure. Because it intended to define a distinct offense for conspiracy in subsection (a)(5), Congress must also have intended to define distinct offenses in subsections (a)(1) through (a)(3). *See United States v. Summit Refrigeration Group, Inc.*, 2006 WL 3009111 (E.D. Wisc. Oct. 26, 2006) ("the plain language of 18 U.S.C. § 1832 does not . . . suggest that Congress intended that there be just one penalty for violating any one or more of the subsections contained therein").

Even if Counts Ten and Eleven were multiplicitous, the wholesale dismissal of both

counts would amount to throwing the baby out with the bath water. The remedy for meritorious multiplicity claims is for the district court to vacate the multiplicitous conviction and sentence. *United States v. Zalapa*, 509 F.3d 1060, 1065 (9th Cir. 2007); *accord Ball v. United States*, 470 U.S. 856, 864 (1985); *United States v. Luskin*, 926 F.2d 372, 378 (4th Cir. 1991).[6] Accordingly, the defendant's motion to dismiss those counts must be denied.

V. THE MAIL FRAUD CHARGES PROPERLY STATE AN OFFENSE.

The defendant's final argument is that the mail fraud charges in the Indictment should be dismissed because "an undisclosed breach of an invalid contractual provision does not constitute fraud." Def. Mtn., at 12. The defendant's argument fails for two reasons.

First, the Indictment alleges much more than an "undisclosed breach" of contract, and much more than a breach of what Nosal calls the "non-compete" provisions of his agreement with Korn/Ferry. Rather, as set out in more detail below, it alleges that Nosal devised a scheme to defraud Korn/Ferry through theft of proprietary and confidential information from its computer system, regular misrepresentations about his activities, and use of a fictitious name, all the while accepting $25,000 monthly payments from Korn/Ferry that were meant to compensate him for making his best efforts to act in Korn/Ferry's best interests.

Second, Nosal's argument that he could not have defrauded Korn/Ferry because his independent contractor agreement with Korn/Ferry was invalid under Section 16600 of the California Business and Professions Code fails to consider well-settled law holding that the scope of the federal fraud statutes is not confined by state law.

These points are set out in more detail below.

---

[6]To the extent that this Court finds that Count Ten is duplicitous because it charges two offenses in a single count, *see* Def. Mtn., at 11 n.6, dismissal of that count is also not the proper remedy. *See United States v. Ramirez-Martinez*, 273 F.3d 915 (9th Cir. 2001) ("'Defendant's remedy is to move to require the prosecution to elect . . . the charge within the count upon which it will rely. Additionally, a duplicitous . . . indictment is remediable by the court's instruction to the jury particularizing the distinct offense charged in each count in the indictment.'") (quoting *United States v. Robinson*, 651 F.2d 1188, 1194 (6th Cir. 1981)); *see also* 1A Charles A. Wright, *Federal Practice and Procedure: Criminal* § 145 at 83–84 (1999) (duplicity "is not fatal and does not require dismissal of the indictment").

A. The Indictment Alleges a Scheme to Defraud under the Mail Fraud Statute.

A conviction under the mail fraud statute requires the government to prove: (1) a scheme to defraud; (2) use of the mails in furtherance of the scheme; and (3) specific intent to defraud. *See United States v. Selby*, — F.3d —, 2009 WL 102711, at *8 (9th Cir. 2009) (wire fraud). The government agrees that a breach of contract might not, in and of itself, constitute a basis for mail fraud charges. However, the Indictment in this case alleges far more than a simple breach of contract by Nosal. Rather, the Indictment alleges that the defendant devised a scheme to defraud Korn/Ferry that consisted of:

- Nosal's direction to others to steal trade secrets and other things of value from Korn/Ferry's computer system, Indictment, ¶ 28;
- Nosal's use, direction to others to use, and ratification of others' use of trade secrets and other things of value stolen from Korn/Ferry's computer system for the purpose of assisting Nosal's competing business with Korn/Ferry, *id.*, ¶ 29;
- Nosal's deprivation of honest services as an independent contractor to Korn/Ferry, by engaging in business on his own behalf, through shell companies, instead of solely for Korn/Ferry, *id.*, ¶¶ 30–31;
- Affirmative misrepresentations by Nosal on numerous occasions to Korn/Ferry executives that he was complying with his agreement with Korn/Ferry, for the purpose of defrauding Korn/Ferry into continuing to make $25,000 monthly payments, among other payments, *id.*, ¶ 32;
- Nosal's failure to notify Korn/Ferry that he was engaging in his own executive search activities (and thus failure to notify Korn/Ferry that he was no longer entitled to $25,000 monthly stipends), *id.*; and
- Nosal's concealment from Korn/Ferry that he was engaging in his own executive search activities by, for example, using a fictitious name when he interviewed candidates for executive positions that he was seeking to fill, *id.*, ¶¶ 32–33.

The mail fraud charges also incorporate the allegations in ¶¶ 1–11 and ¶¶ 13–19 of the Indictment regarding specific actions taken by Nosal and others to access Korn/Ferry's computer system for the purpose of stealing confidential and proprietary information. The Indictment alleges that, for the purpose of executing and attempting to execute this scheme to defraud, the defendant caused eight (8) $25,000 checks to be mailed by Korn/Ferry to his home in this District. These mailings are alleged in Counts Twelve through Nineteen.

None of the cases cited by the defendant in which the courts found a breach of contract to

be insufficient to support mail fraud charges, *see* Def. Mtn., at 13, involved situations involving such extensive schemes to defraud. *See, e.g.*, *Kehr Packages v. Fidelcor, Inc.*, 926 F.2d 1406, 1417 (3d Cir. 1991) (holding that allegation that defendant "unreasonably delayed" approving sale of corporation to plaintiffs, while possibly amounting to breach of contract, "contains no deception that would bring it within the purview of the mail fraud statute"); *McEvoy Travel Bureau, Inc. v. Heritage Travel, Inc.*, 904 F.2d 786, 792 (1st Cir. 1990) (holding that allegations of complaint did not sufficiently allege scheme to defraud any entity of money or property).[7] Accordingly, the detailed allegations of this Indictment distinguish this case from the cases relied upon by the defendant.

The defendant deftly sidesteps the portions of the Indictment that allege that, as part of the scheme to defraud, Nosal stole proprietary and confidential information from Korn/Ferry and "affirmatively misrepresented on numerous occasions to Korn/Ferry executives that he was complying with the Nosal-Korn/Ferry Agreements." Indictment, ¶¶ 28–29, 32. This is telling, because such allegations, if true, clearly establish that Nosal's actions constituted more than a simple breach of contract.

Nosal's argument that the Indictment is insufficient because it fails to allege that he intended to cause economic harm to Korn/Ferry is also without merit. *See* Def. Mtn., at 13–14 (citing *Pennington* and *Sun-Diamond Growers*). Neither case cited by the defendant holds that an Indictment must contain such allegations, which allegations are not elements of the mail fraud offense. In any event, the Indictment *does* contain such allegations because it alleges that the defendant engaged in a scheme to defraud Korn/Ferry for the purpose of receiving "monthly independent contractor payments of $25,000 from Korn/Ferry and so that he remained eligible to

---

[7]Beyond the allegations of the Indictment here (which sufficiently allege the elements of the mail fraud statute), the government intends to prove at trial that, *prior* to entering into his agreement with Korn/Ferry, the defendant began directing others to take materials from Korn/Ferry in preparation for starting a competing business. *See, e.g.*, Plea Agrm., ¶ 2, CR 07-0568 MHP (docket entry 9) ("I also understood [Nosal] to be directing me to take from Korn/Ferry whatever I thought would be necessary or helpful for [Nosal's] new company, including 'source lists' to populate the database at [Nosal's] new company.").

be paid the lump-sum payments" envisioned in the parties' agreement and because it alleges that he stole valuable information from Korn/Ferry. Indictment, ¶¶ 28–29, 32.

In sum, although the mail fraud statute may not reach every business practice that fails to fulfill expectations, every breach of contract, or every breach of fiduciary duty, it *does* reach such breaches where there was a recognizable scheme to defraud and where the defendant has made fraudulent representations or omissions reasonably calculated to deceive. The allegations in the pending Indictment describe such a scheme, and, for that reason, the defendant's motion should be denied.

B. California Law Does Not, and Cannot, Preclude the Mail Fraud Charges.

The defendant's argument that the mail fraud counts must be dismissed because California law prohibits "noncompetition" agreements is without merit. *See* Def. Mtn., at 14–15 (relying on California Business and Professions Code 16600).

As an initial matter, the agreement between Nosal and Korn/Ferry was not a "noncompetition" agreement falling within the prohibitions of Section 16600. (Indeed, even the defendant is careful not to label the entire agreement as a "noncompetition" agreement, but only argues that the agreement contains "non-compete" provisions. Def. Mtn., at 12:23–25.) Rather, it was an agreement in which Nosal agreed to act solely as an independent contractor to Korn/Ferry for a period of one year. In addition, that agreement contained other promises on Nosal's behalf, including promises to maintain the confidentiality of the information in Korn/Ferry's computer system. *See* Def. Mtn., Ex. 1, ¶ 18, at 9. In return for *all* of the promises he made, Nosal received the sizable salary of $25,000 per month, in addition to being eligible to receive lump-sum payments from Korn/Ferry near the end of his term as independent contractor. The defendant has cited no California law that makes such an arrangement requiring a duty of loyalty on the part of a compensated independent contractor void or invalid. The California Supreme Court's decision in *Edwards v. Arthur Andersen LLP*, 44 Cal. 4th 937 (2008), a case heavily relied upon by the defendant, is not to the contrary. The agreement in that case was a pure "noncompetition" agreement that restricted the employee's ability to work for or solicit particular clients after he left Arthur Andersen's employment. *See id.* at 942. The agreement in

Edwards did not involve, as did the agreement here, a continued quasi-employment relationship between the parties.

Notably, by its very terms, Nosal's agreement with Korn/Ferry did not run afoul of Section 16600 because it did not restrain him from engaging in a lawful profession, trade, or business. *At any time*, Nosal could have withdrawn from the agreement and conducted his own executive search activities. In doing so, however, he would have become ineligible to receive the $25,000 monthly payments, or the lump-sum payments, that Korn/Ferry agreed to pay in return for Nosal agreeing to work solely for Korn/Ferry, payments which Korn/Ferry was not otherwise bound to pay him.

Even assuming that the independent contractor agreement that Nosal voluntarily entered into with Korn/Ferry was void under California law, that situation would not require dismissal of the mail fraud charges. The Ninth Circuit has held that "'state law is irrelevant in determining whether a certain course of conduct is violative of the wire fraud statute.'" *United States v. Weyhrauch*, 548 F.3d 1237, 1245 (9th Cir. 2008) (quoting *United States v. Louderman*, 576 F.2d 1383, 1387 (9th Cir. 1978)); *see also Weyhrauch*, 548 F.3d at 1245 (noting that Ninth Circuit has "never limited the reach of the federal fraud statutes only to conduct that violates state law") (honest services mail fraud prosecution of public official).[8] Although these cases consider state law under different circumstances than in this case, they enunciate the general principle that federal mail fraud prosecutions should not be conditioned on the vagaries of state law.

Moreover, despite the defendant's arguments regarding "federalism," "federal action based on a valid constitutional grant of authority is not improper simply because it intrudes on state interests." *Weyhrauch*, 548 F.3d at 1246. The Supreme Court's decision in *Cleveland v. United States*, 531 U.S. 12 (2000) — cited by the defendant — does not hold otherwise. In *Cleveland*, the Court simply held that the state licenses at issue were not "property" falling within the scope of the mail fraud statute. *Id.* at 20.

---

[8]The Ninth Circuit expressed "no opinion" on the role of state law in honest services fraud prosecutions in the private context. *Weyhrauch*, 548 F.3d at 1237 n.5.

* * *

A *breach of contract* occurs with a failure to perform, but *fraud* occurs when the breaching party induces payment by falsely representing that he has performed under the contract. This Indictment alleges that the defendant David Nosal entered into an agreement with his employer, Korn/Ferry, to act as an independent contractor for one year after he left formal employment with Korn/Ferry. As part of that agreement, Nosal agreed to work only on behalf of Korn/Ferry. In return for Nosal's promises, Korn/Ferry promised to pay, and did pay (until after it learned of his fraud), $25,000 per month to Nosal. However, as the Indictment alleges, Nosal *did not* put all of his efforts into working only on behalf of Korn/Ferry, and garnered some $500,000 working on his own behalf through Christian & Associates. *See* Indictment, ¶ 30. All the while, the Indictment alleges, Nosal affirmatively lied to Korn/Ferry about his activities, used a fictitious name in conducting his business, and stole information from Korn/Ferry in order to assist that business. The allegations, if true, constitute part of a scheme to defraud. For these reasons, and for all of the reasons set forth above, the Court should deny the defendant's motion to dismiss the mail fraud charges in the Indictment.

CONCLUSION

For all of the reasons stated above, the United States respectfully requests that the Court deny the defendant's motion to dismiss in its entirety.

DATED: February 2, 2009

Respectfully submitted,

SCOTT N. SCHOOLS
Acting United States Attorney

/s/
KYLE F. WALDINGER
Assistant United States Attorney